c) establishing a second stream between the second process and the communication channel;

d) in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol[s] layers used to transport the encrypted data from the first network node to the second network node;

e) causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

f) in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocol[s] layers used to transport the encrypted data from the first network node to the second network node.

2. (AMENDED) The method of Claim 1, further including the steps of

a) performing a communication protocol[-] layer specific encryption of the data on the first network node, and

b) performing a communication protocol[-] layer specific decryption of the data on the second network node.

4. (AMENDED) The method of Claim 1, wherein the communication channel is a Java secure channel, wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the method further comprises the step of connecting the Java secure channel to a third Java stream, and

wherein the third Java stream provides for the transmission of data according to a specific communication protocol layer.

5. (AMENDED) A computer-readable medium carrying one or more sequences of one or more instructions for providing communication protocol[-] layer independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, wherein the first network node and the second network node each support at least one common communication protocol layer, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

a) establishing a communication channel between the first network node and the second network node;

b) establishing a first stream between the first process and the communication channel;

c) establishing a second stream between the second process and the communication channel;

d) in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol[s] layers used to transport the encrypted data from the first network node to the second network node;

E2

e) causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

D2 cont

f) in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data from the first network node to the second network node.

6. (AMENDED) The computer-readable medium of Claim 5, wherein the computer-readable medium further includes instructions for performing the steps of

a) performing a communication protocol[-] layer specific encryption of the data on the first network node, and

b) performing a communication protocol[-] layer specific decryption of the data on the second network node.

D3

8. (AMENDED) The computer-readable medium of Claim 5, wherein the communication channel is a Java secure channel,

wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the computer-readable medium further includes instructions for connecting the Java secure channel to a third Java stream, and

wherein the third Java stream provides for the transmission of data according to a specific communication protocol layer.

13. (AMENDED) A computer data signal embodied in a carrier wave and representing sequences of instruction which, when executed by one or more processors, provide communication protocol[-] layer independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, according to at least one common communication protocol layer supported by the first and second network nodes, by performing the steps of:

a) establishing a communication channel between the first network node and the second network node;

b) establishing a first stream between the first process and the communication channel;

c) establishing a second stream between the second process and the communication channel;

d) in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol[s] layers used to transport the encrypted data from the first network node to the second network node;

e) causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

f) in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocol[s] layers used to transport the encrypted data from the first network node to the second network node.

14. (AMENDED) The computer data signal of Claim 13, wherein the computer sequence of instructions further includes instructions for performing the steps of

a) performing a communication protocol[-] layer specific encryption of the data on the first network node, and

b) performing a communication protocol[-] layer specific decryption of the data on the second network node.

16. (AMENDED) The computer data signal of Claim 13, wherein the communication channel is a Java secure channel,

wherein the first stream is a Java stream,

wherein the second stream is a Java stream,

wherein the computer sequence of instructions further includes instructions for connecting the Java secure channel to a third Java stream, and

wherein the third Java stream provides for the transmission of data according to a specific communication protocol layer.

17. (AMENDED) A method for providing communication protocol[-] layer independent security for data transmitted by a process executing on a network node, the method comprising the steps of:

a) establishing a stream between the process and a communication channel; and

b) in response to the data being written to the stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication[s] protocol layers used to transport the encrypted data on the communication[s] channel.

18. (AMENDED) The method of Claim 17, wherein the communication[s] channel is a Java secure channel,

wherein the stream is a first Java stream, and

wherein the step of establishing a stream between the process and the communication[s] channel further comprises the step of establishing a Java stream between the process and the Java secure channel.

19. (AMENDED) The method of Claim 17, wherein the communication channel is a Java secure channel, wherein the stream is a Java stream,

wherein the method further comprises the step of connecting the Java secure channel to a second Java stream, and

wherein the second Java stream provides for the transmission of data according to a specific communication protocol layer.

Please add new claims 20-35.

--20. A method for providing communication protocol-independent security for data transmitted between a first node and a second node, the method comprising the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel in response to the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process in response to the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

21. The method of claim 20, wherein the encryption of the first stream and the decryption of the second stream is specific to a communication protocol layer.

22. The method of claim 20, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream after the first process and before the communication channel further comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream after the communication channel and before the second process further comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

23. The method of claim 20, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream

the method further comprises the step of connecting the the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

24. A computer-readable medium carrying one or more sequences of one or more instructions for providing communication protocol-layer independent security for data transmitted between a first node and a second node, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel in response to the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process in response to the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

25. The computer-readable medium of claim 24, wherein the encryption of the first stream and the decryption of the second stream is specific to a communication protocol layer.

26. The computer-readable medium of claim 24, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream after the first process and before the communication channel further comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream after the communication channel and before the second process further comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

27. The method of claim 24, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

28. A communications network providing communication protocol-independent security for data transmitted between a first node and a second node, the communication network performing the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel in response to the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process in response to the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

29. The communication network of claim 28, wherein the encryption of the first stream and the decryption of the second stream is specific to a communication protocol layer.

30. The communication network of claim 28, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream after the first process and before the communication channel further comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream after the communication channel and before the second process further comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

31. The communication network of claim 28, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

32. A computer data signal embodied in a carrier wave and representing sequences of instructions which, when executed by one or more processor, provide communication protocol-independent security for data transmitted between a first node and a second node, by performing the steps of:

establishing a communication channel between a first network node and a second network node;

establishing a first stream from a first process to the communication channel in response to the establishment of the communication channel, wherein the first stream is encrypted after the first process and before entering the communication channel and the encrypted first stream is independent of any communication protocol layers; and

establishing a second stream from the communication channel to a second process in response to the establishment of the communication channel, wherein the second stream is decrypted after the communication channel and before entering the second process.

33. The computer data signal of claim 32, wherein the encryption of the first stream and the decryption of the second stream is specific to a communication protocol layer.

34. The computer data signal of claim 32, wherein:

the first stream is a first Java stream;

the second stream is a second Java stream;

the step of establishing a communication channel between the first network node and second network node further comprises the step of establishing a Java secure channel between the first network node and second network node;

the step of establishing the first stream after the first process and before the communication channel further comprises the step of establishing the first Java stream after the first process and before the Java secure channel; and

the step of establishing a second stream after the communication channel and before the second process further comprises the step of establishing the second Java stream after the Java secure channel and before the second process.

D6 cont

35. The computer data signal of claim 32, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream

the method further comprises the step of connecting the Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.--

REMARKS

Claims 1-8 and 13-35 are pending in the application. Claims 1-2, 4-6, 8, 13-14, and 16-19 are amended in response to the Examiner's Official Action dated January 28, 2000. New claims 20-35 have been added.

Claims 1, 2, 5, 6, 13, and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Gillon et al., U.S. Patent 5,838,927, in view of Elgamal et al., U.S. Patent 5,657,390, Shaffer et al., U.S. Patent 5,784,461, and either Finkelstein et al., U.S. Patent 5,319,712 or Zuquete et al. This rejection is respectfully traversed. The following is a comparison between applied reference and the claimed invention.

The present invention relates to a method for providing communication protocol layer independent security for data transmitted between two network nodes. The method